在线支付及风险防范实务

支付宝（中国）网络技术有限公司

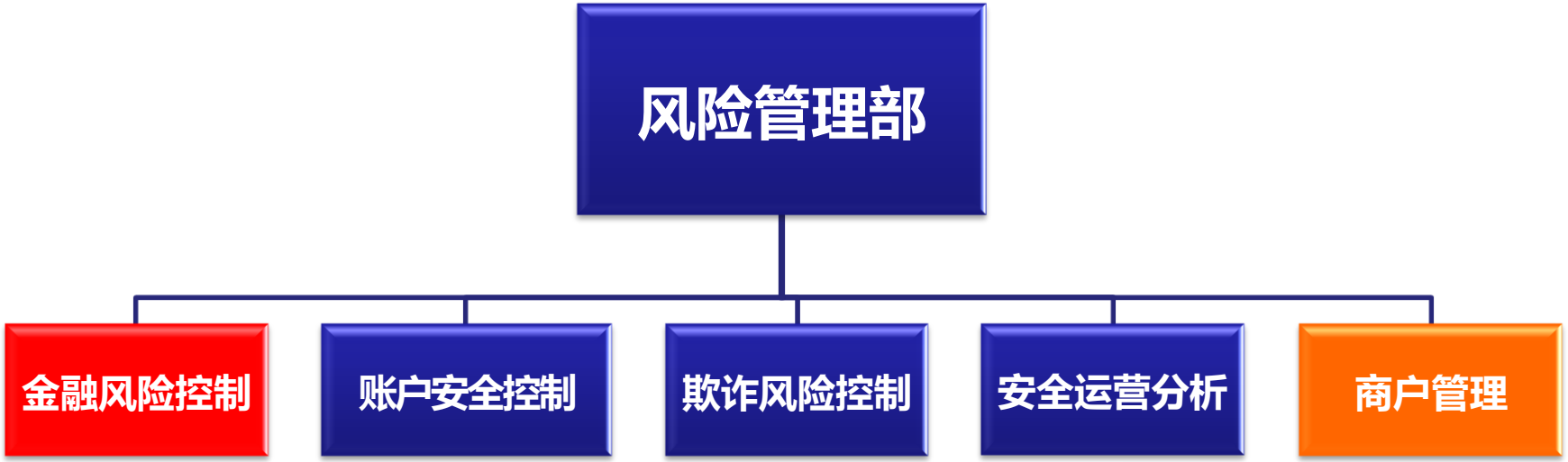
风险管理部

2010.09

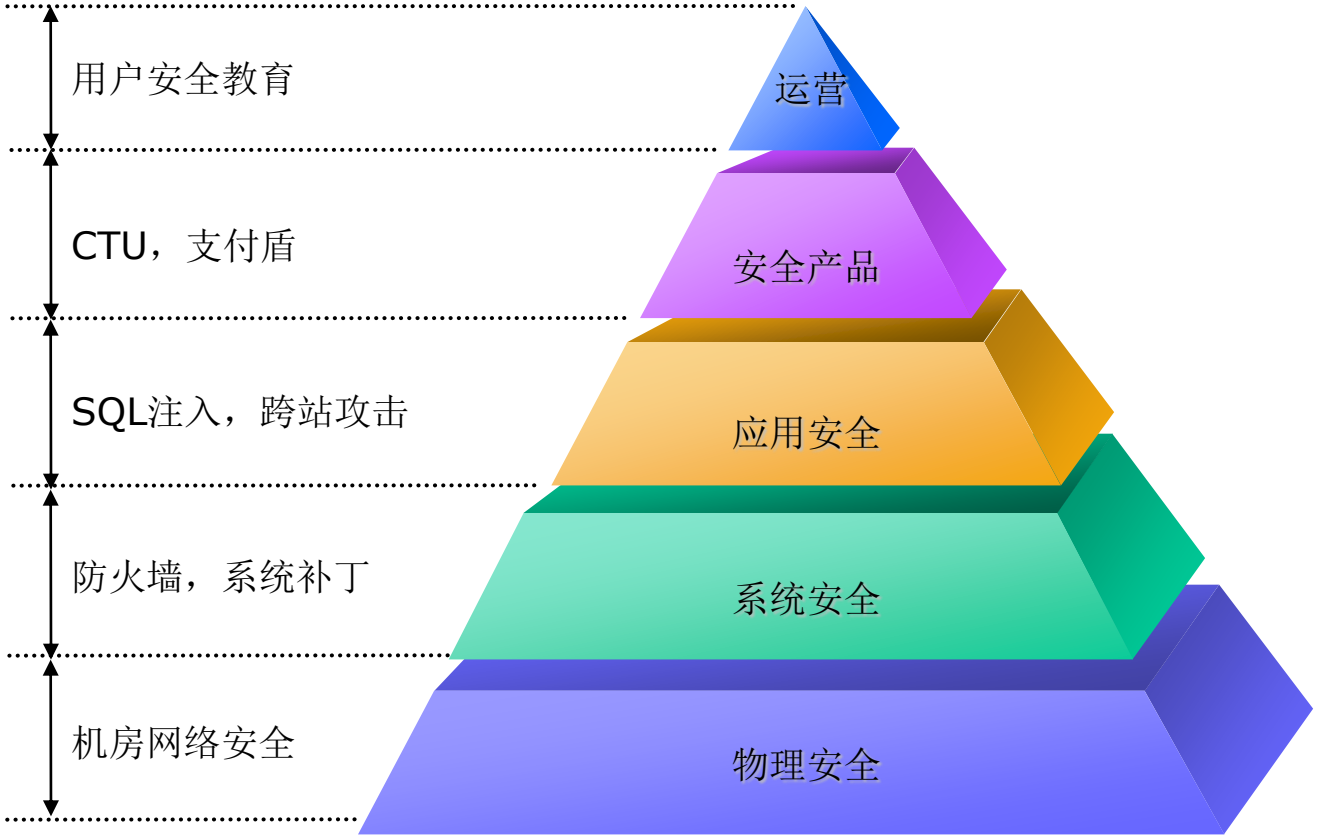
概述

- 支付宝风险管理架构
- 信用卡套现风控措施
- 银行卡盗用风控措施
- 信用卡大额支付风控措施
- 商户风险管理
- 反洗钱工作概览

支付宝风险管理架构——组织架构



支付宝安全体系



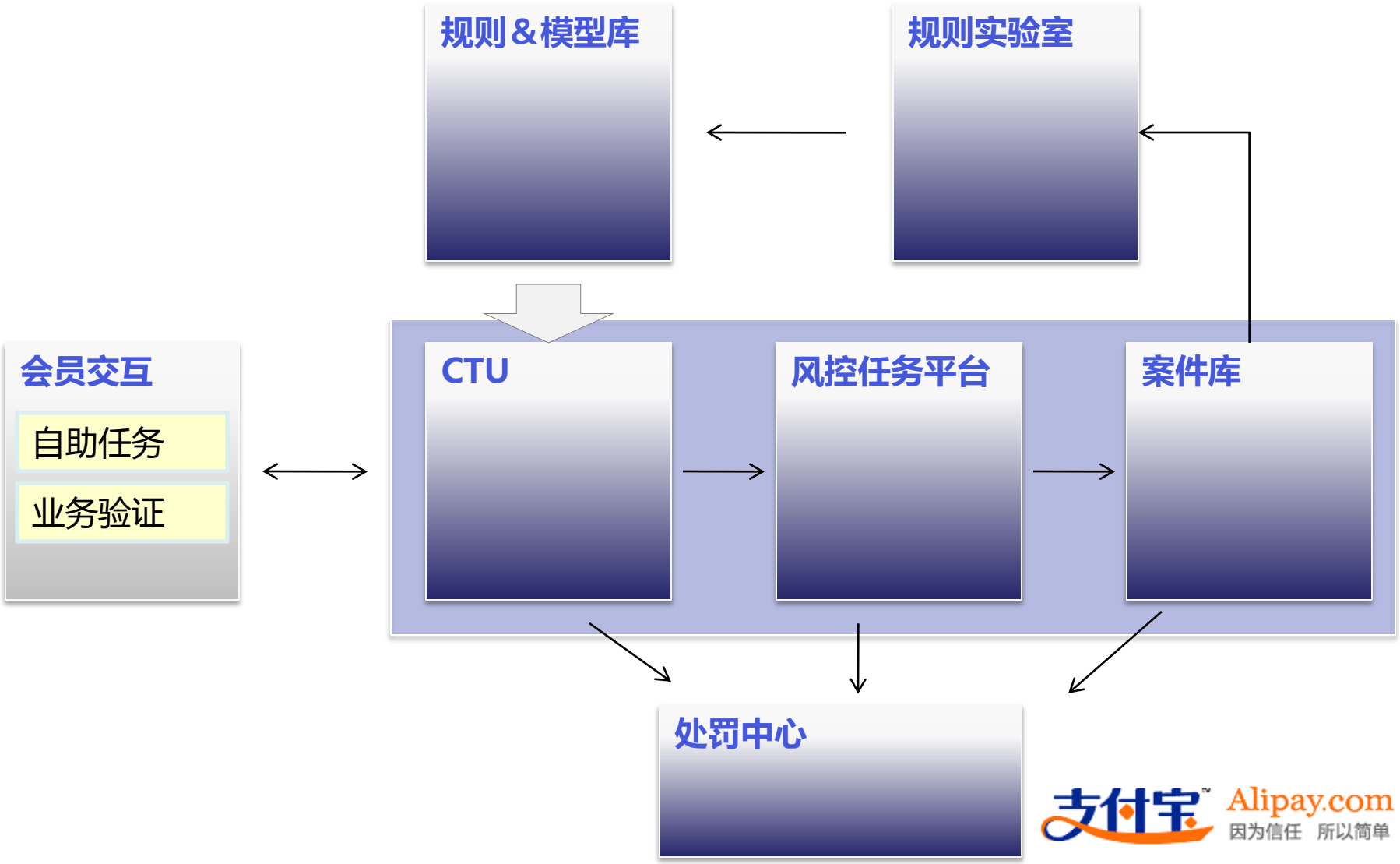
支付宝风控体系

- 安全控件
- 支付盾
- 数字证书
- 手机动态口令
- 安全教育
- 支付宝工具条
- 钓鱼头像

- 用户权限控制
- 交易额度控制
- 风控名单库
- 安全检测

- CTU分析引擎
- 增强身份认证
- 安全模型
- 规则维护
- 规则监控/自学习
- 规则运行分析
- 机器识别

风控业务流



网络安全运营

1. 金山：安全整体合作项目(反钓鱼识别，客户端产品
2. RSA：IE反钓鱼屏蔽功能
3. Mark Monitor：反钓鱼网址浏览器屏蔽服务
4. ESET：代扣功能和活动
5. 遨游： 恶意网站警告

1. 163免费邮箱
2. Hotmail邮箱
3. Gmail邮箱
4. Tom邮箱

支付宝ESU（是支付宝公司常设的跨部门协作应对突发事件的团队。

反钓鱼邮件

支付宝 Alipay.com
因为信任 所以简单

PCI DSS认证

- **支付卡行业与数据安全标准**
- **12项国际数据安全标准**
- **与TRUSTWAVE开展PCI DSS认证项目**

图片来源：Novell

风险管理体系

- 风险核查管理规定
- 风险监测系统规则管理理规定
- 银行卡被盗处理流程
- 信用卡套现处理流程
- 商户准入标准及管理办法

信用卡套现风险控制措施

信用卡套现风险控制措施

事前

- **支付宝信用体系**
- **用户教育及宣传**
- **支付宝信用模型评分，实名认证，关闭卖家收款功能。**

事中

- **CTU风险控制系统**
- **数据分析和数据挖掘，套现行为特征，建立反套现规则监控**

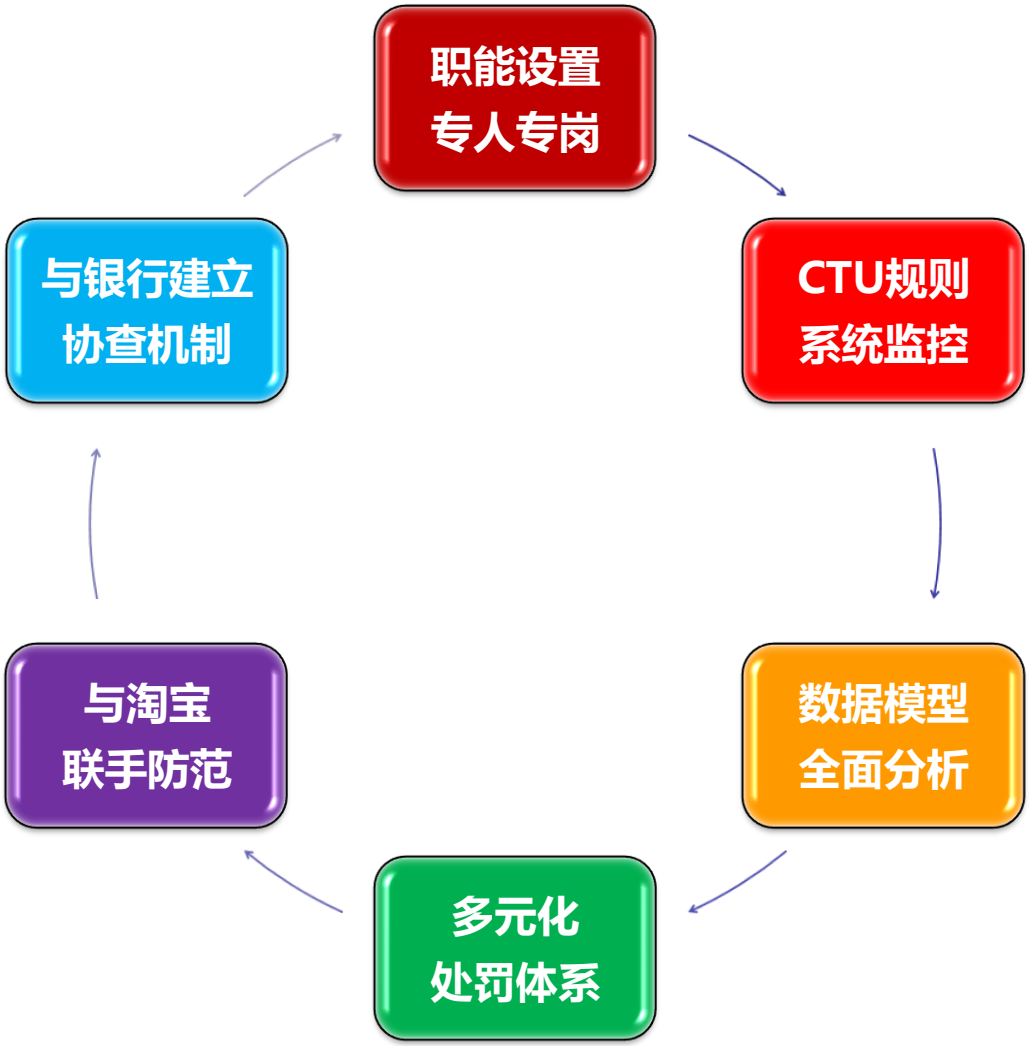
事后

- **处理套现账户**
- **邮件警告　关闭收款功能　冻结账户　关闭卖家功能**

（四）其他措施

- 支付宝账户实名认证制度
- 提现金额计算逻辑
- 社区论坛套现不良信息屏蔽
- 支付宝站内交易收费
- 维护套现黑名单

套现事中控制



支付宝套现核查流程

◈ 数据来源

- 信用模型预警
- CTU风险监测系统
- 内、外部各种举报

◈ 处理流程

- 对认定为套现的账户，限制其相关功能。邮件通知其提供交易凭证以证明交易的真实性。
- 根据核查期内与会员互动的情况，在核查期结束时，进行相应处理，并以邮件通知会员。
- 采用黑名单库的形式进行后续的跟踪和关注。

信用卡套现风控措施—打击套现成效

30	数据模型应用近30个模型逻辑节点, 追踪用户完成套现的所有的行为。
60	数据模型提供60多个相关的嫌疑数据参考字段。
∑	数据模型进行多维度分析、多重条件组合，几乎覆盖所有套现方式和途径
98%	套现数据抓捕准确率高达98%以上
>1000	支付宝日处罚能力可达数千个账户
>8	风控、客服、运营、技术、金融合作、公关、淘宝、阿里软件等多部门、多公司的协作 。

银行卡盗用风险控制措施

银行卡盗用风险控制措施

建立联系

- 签定保密协议
- 双方指定联系人
- 明确协查流程
- 为银行协查
- 主动向银行反馈

若有资金截留，凭银行提供的《退款公函》支付宝将资金直接退回银行卡账户中。

信息互换

- 可疑IP地址
- 可疑银行卡号
- 可疑身份证号
- 可疑订单号
- 可疑手机号码

建立信息互换机制，可以有效地打击盗卡行为，最大限度地减少持卡人资金损失，将银行卡案件控制在交易过程中。

事后补救

- 案件跟踪处理
- 案件反查
- 黑名单
- 数据分析
- CTU规则调整

信用卡大额支付风险控制

信用卡大额支付风险控制

1、准入的商户类型及条件，接入网关的商户必须同时满足如下要求。

- 必须是经营实物类或实名消费类商户。有经营网站或网店，且网站或网店运行情况良好，系统稳定，无欺诈投诉。
- 必须已加入淘宝消费者保障计划的商户。
- 在淘宝开店时间超过12个月，信用度三钻及以上，并且好评率大于98%。
- 最近12个月内无“炒作信用、套现”等违规核查记录。

2、禁入商户类型：

- 预付款类型商户，虚拟商品类型商户（如点卡、充值卡）。
- 珠宝、古玩等易于套现及销赃行业。
- 其他支付宝认定高风险类型行业的商户。

3、接入网关后，定期核查发现如下行为的商户实施强制退出机制（非合同因素关闭）

- 经核查，支付宝认定有“炒作信用、套现”等违规行为的。
- 长期无交易，网站无经营活动的。
- 发生网站接口被盗用，自身风险防范能力低的。

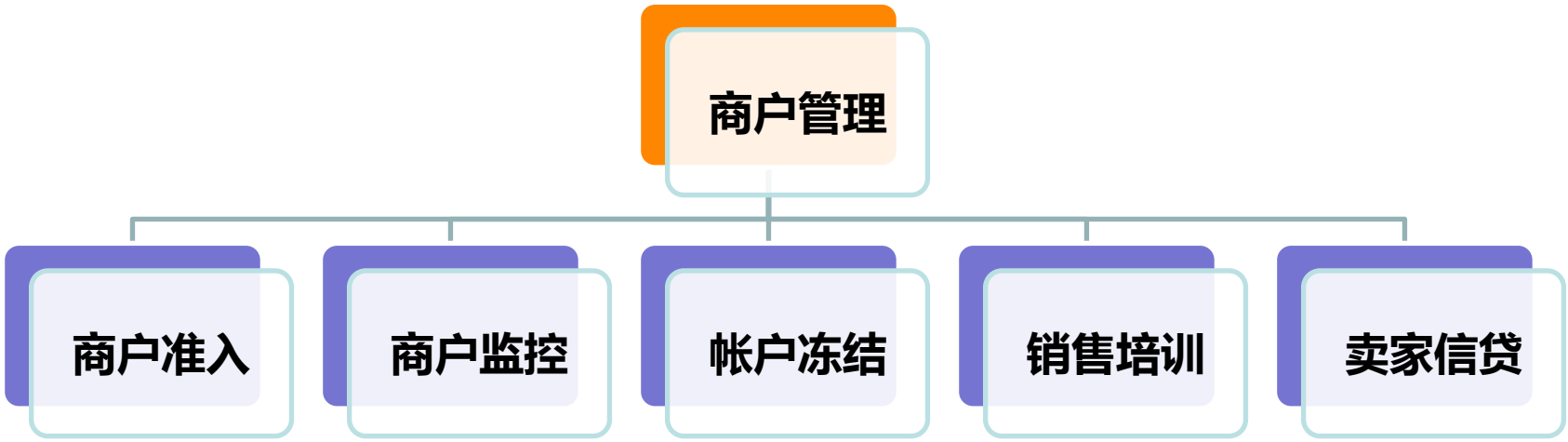
信用卡大额支付风险控制---套现控制

- 1、交易收费管理。大额网关项目对商家实施收费，提高网上交易成本，在一定程度上能够有效遏制套现发生。
- 2、商户严进严管。对接入大额信用卡网关的网上商户进行“严进严管”，有专门的团队负责定期和不定期对接入商户进行核查，一旦发现违规立即实施强制退出机制。
- 3、虚假交易冲退。支付宝风险监控系统对网上交易实时监控，拦截虚假可疑交易，同时辅以人工核查、接受举报等方式全方位追踪虚假交易，一旦发现套现交易，就进行支付订单冲退操作，交易资金原路退回到付款信用卡。
- 4、只能用于消费。大额信用卡网关只能用于网上消费支付，不能向支付宝账户充值，能够有效阻止套现途径。

商户管理

商户管理团队

- **成立于2007年10月**



商户风险

商户准入审核要点

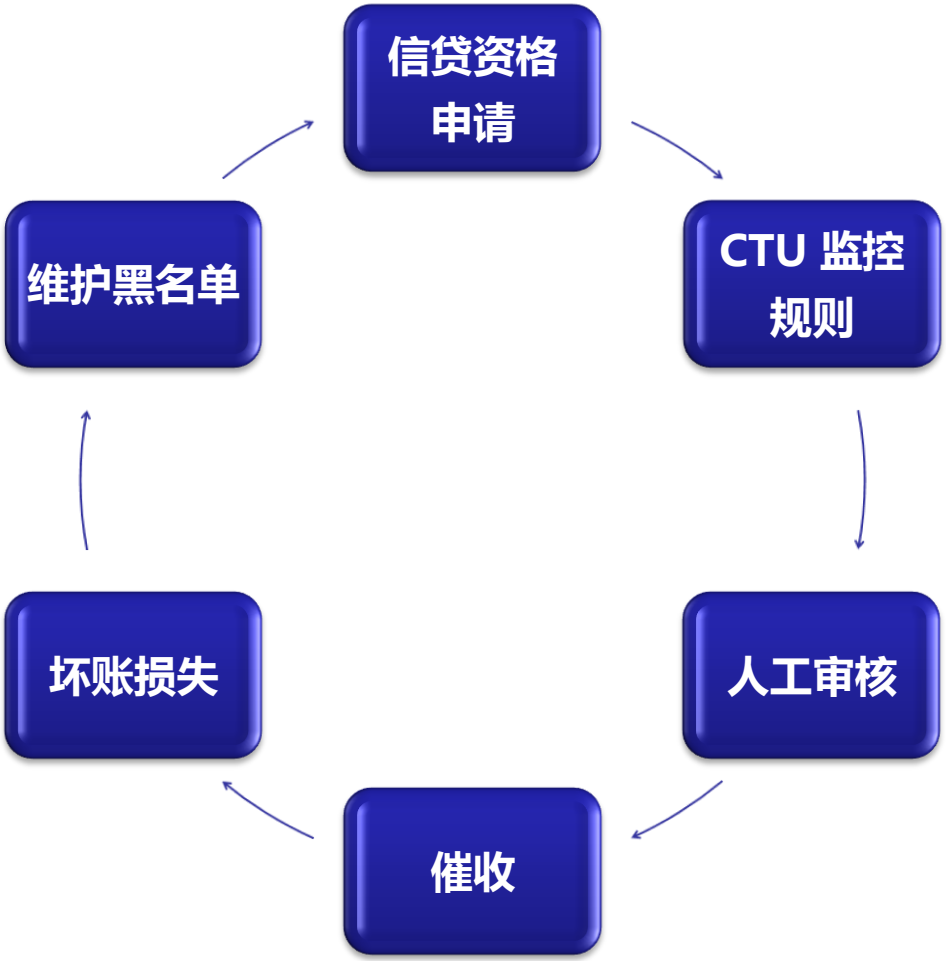
1. 身份信息实名认证
2. 银行卡信息认证
3. 网站浏览
4. 内部反欺诈数据库过滤
5. 营业执照审核
6. 经营范围
7. 高风险行业/特殊行业准入要求
8. 培训销售团队-商户风险手册
9. 。。。

商户管理流程

商户事中审核

- Top 100 交易量商户定期核查
- 交易量及签约量消耗比值监控
- 违禁品关键字的搜索引擎
- 大额交易量，交易增长超过150%商户的人工审核
- 高危商户定期审查
- 商户上门拜访
- CTU规则系统

卖家信贷管理



商户风险管理平台

一个集中所有商户处理任务的平台

设置工作流，风险事件根据分类自动分流

记录核查信息等备注信息供将来使用

与客户签约系统打通，实现数据同步

统计及报告功能

反洗钱工作

反洗钱义务

- 客户身份识别（KYC）
- 大额可疑交易核查
- 定期向监管部门提交反洗钱报告
- 相关记录保存

客户身份识别

KYC：Know Your Customer
（了解你的客户）

准入商户前，了解掌握对方的基本信息，包括主营业务，注册地，是否法人，通讯地址等。

准入商户后，根据支付宝内部准则进行商户洗钱风险分级，并定期进行各项数据的审查，防范潜在洗钱风险。

大额可疑交易核查

大额和可疑交易报告

客观性报告----大额交易报告

- 筛选出所有在一定金额以上的交易，逐笔进行人工核查

主观性报告----可疑交易报告

- 通过内部黑名单&可疑关注名单对数据进行过滤
- 对过滤出具有一定风险的交易进行人工核查并记录

大额可疑交易上报

每月制作大额可疑交易报告（包括账户、银行卡及交易等信息）

向当地监管部门（人民银行）进行上报

维护合作金融机构权益，履行反洗钱职责和义务

相关记录保存

记录保存

5年

安全 准确

完整 保密

建议与银行的合作事项

建议合作的事项

- 银行与支付宝共同开展网上支付用户教育，增强用户风险防范意识
- 银行与支付宝建立黑名单共享机制，提前预防盗卡，套现交易，减少资金损失
- 加强双方风控人员的沟通交流，借鉴双方经验，共同维护健康的在线支付环境